line 30, delete "that" and insert therefor --wherein--.

Claim 17, page 15, line 2, delete "(2, 3)";
line 3, delete "(1)" and "(5)"; and
line 4, delete "characterised by" and insert therefor --comprising--.

Claim 18, page 15, line 18, delete "characterised by" and insert therefor --comprising--;
line 17, delete "(6)";
line 21, delete "(1)";
line 23, delete "(1)";
line 25, delete "(1)"; and
line 27, delete "(5)".

Claim 19, page 15, line 30, delete "(6)";
line 33, delete "(1)"; and
line 35, delete "(1)".
page 16, line 2, delete "(1)"; and
line 4, delete "(5)".

"Express Mail" mailing label No. EL581399724US
Date of Deposit 9/29/00
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.
H. Rattelade
(Type or printed name of person mailing paper or fee)
(Signature of person mailing paper or fee)

REMARKS

The written description and claims have been amended and the Abstract has been replaced to place the application in better form for examination. Favorable consideration is respectfully solicited.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

P.O. Box 1404
Alexandria, Virginia 22313-1404
(919) 941-9240

By: Michael G. Savage
Registration No. 32,596

Dated: September 29, 2000

ABSTRACT

A method for executing secure data transfer between a communication device and an application server in a wireless network, in which a request requiring a secure transaction of data is sent from either the communication device or the server. An agreement proposal for the secure transaction is sent to the communication device, and if the agreement proposal is considered acceptable, the agreement proposal is sent to a security adapter. Details of the transaction are entered into a message and sent to a smart card in order to activate a signing application in the smart card. The details of the transaction are displayed on the communication device, and if the transaction is accepted, the signing application signs the data and sends it to the security adapter via messages, the signature is verified, and the data is sent to the server.